



UNITED STATES PATENT AND TRADEMARK OFFICE

(Handwritten mark)

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/458,921	12/10/1999	MOHAMMAD PEYRAVIAN	P-4541.001	9480
24112	7590	08/18/2006	EXAMINER	
COATS & BENNETT, PLLC P O BOX 5 RALEIGH, NC 27602			MOORTHY, ARAVIND K	
			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 08/18/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

DETAILED ACTION

1. This is in response to the amendment filed on 2 June 2006.
2. Claims 1-52 are pending in the application.
3. Claims 29-46, 51 and 52 have been rejected.
4. Claims 1-28 and 47-50 have been allowed.

Response to Arguments

5. Applicant's arguments with respect to claims 29-46, 51 and 52 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 29-46, 51 and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pasioka U.S. Patent No. 6,587,945 B1 in view of Applied Cryptography (hereinafter Schneier).

As to claim 29, Pasioka discloses a method for time stamping a document comprising:

- a. receiving a time stamp request at an outside agency at a first time, the time stamp request including identifying data associated with the document [column 5 line 4 to column 6 line 14];
- b. creating at the outside agency a time stamp receipt based on the identifying data and a time indication [column 5 line 4 to column 6 line 14]; and

Art Unit: 2131

c. generating at the outside agency a message authentication code based on the time stamp receipt and a public key [column 5 line 4 to column 6 line 14]; and

d. transmitting the time stamp receipt and the message authentication code to the requestor [column 5 line 4 to column 6 line 14].

Pasieka teaches that the message authentication code is based on the time stamp receipt and a public key, not a secret key.

Schneier teaches the benefits of asymmetric (secret) key system over a public key system [page 216].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Pasieka so that the message authentication code would have been based on the time stamp receipt and a secret key, not a public key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Pasieka by the teaching of Schneier because symmetric cryptography is best for encrypting data. It is orders of magnitude faster and is not susceptible to chosen-ciphertext attacks [page 216].

As to claim 30, Pasieka teaches that the identifying data comprises a digital representation of at least a portion of the document [column 5 line 4 to column 6 line 14].

As to claim 31, Pasieka teaches that the identifying data comprises a digital sequence derived by application of a deterministic function to at least a portion of the document [column 5 line 4 to column 6 line 14].

Art Unit: 2131

As to claim 32, Pasioka teaches that the digital sequence is a hash value derived by application of a one-way hashing function to at least a portion of the document [column 5 line 4 to column 6 line 14].

As to claim 33, Pasioka teaches that the time stamp receipt includes a copy of at least a portion of the identifying data concatenated with the time indication [column 7, lines 10-29].

As to claim 34, Pasioka teaches that the time stamp receipt includes a digital sequence derived from the identifying data concatenated with the time indication [column 7, lines 10-29].

As to claim 35, Pasioka teaches that the time stamp request further includes an identification number associated with the requestor [column 8, lines 31-49].

As to claim 36, Pasioka teaches that the message authentication code comprises a numeric representation generated by application of a deterministic function to the time stamp receipt and the secret key concatenated together [column 7, lines 10-29].

As to claim 37, Pasioka teaches generating a second message authentication code based on the first message authentication code and a second secret key [column 7, lines 10-29].

As to claim 38, Pasioka teaches transmitting the second message authentication codes to the requestor [column 7, lines 10-29].

As to claim 39, Pasioka teaches the step of encrypting the first secret key to generate an encrypted key [column 9, lines 1-21].

As to claim 40, Pasioka teaches transmitting the encrypted key to the requestor [column 9, lines 1-21].

As to claim 41, Pasioka discloses a method for time stamping documents comprising:

- a. receiving at an outside agency a certification request, the certification request including a time stamp receipt and a message authentication code generated on the time stamp receipt [column 5 line 4 to column 6 line 14];
- b. validating the message authentication code at the outside agency using a public key [column 5 line 4 to column 6 line 14];
- c. certifying the time stamp receipt if the message authentication code is valid using a cryptographic signature scheme [column 5 line 4 to column 6 line 14].

Pasioka teaches that the message authentication code is based on the time stamp receipt and a public key, not a secret key.

Schneier teaches the benefits of asymmetric (secret) key system over a public key system [page 216].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Pasioka so that the message authentication code would have been based on the time stamp receipt and a secret key, not a public key.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Pasioka by the teaching of Schneier because symmetric cryptography is best for encrypting data. It is orders of magnitude faster and is not susceptible to chosen-ciphertext attacks [page 216].

Art Unit: 2131

As to claim 42, Pasioka teaches that the step of certifying the time stamp receipt includes signing the message authentication code at the outside agency using a cryptographic signature scheme [column 9, lines 41-52].

As to claim 43, Pasioka teaches that the step of certifying the time stamp record includes signing the time stamp receipt at the outside agency using a cryptographic signature scheme [column 9, lines 41-52].

As to claim 44, Pasioka teaches including the step of transmitting the certified time stamp receipt to the requestor [column 9, lines 41-52].

As to claim 45, Pasioka teaches that certifying the time stamp receipt at the outside agency comprises signing the time stamp receipt with a private signature key [column 9, lines 41-52].

As to claim 46, Pasioka teaches that certifying the time stamp receipt at the outside agency comprises signing the message authentication code with a private signature key [column 9, lines 41-52].

As to claims 51 and 52, the combination teaches that the secret key used to generate the message authentication code at the outside agency comprises a secret key of the outside agency [column 9, lines 41-52].

Allowable Subject Matter

7. Claims 1-28 and 47-50 are allowed.

As to claim 1, prior art does not disclose or fairly teach e. receiving a certification request at the outside agency at a second time, the certification request including the time stamp receipt and the message authentication code. Prior art does not disclose or fairly teach f. validating the message authentication code at the outside agency using the secret key. Prior art does not disclose or fairly teach g. certifying the time stamp receipt at the outside agency using a cryptographic signature scheme if the message authentication code is valid.

As to claim 15, prior art does not disclose or fairly teach d. encrypting the first secret key with a second secret key to generate a key message. Prior art does not disclose or fairly teach e. generating a second message authentication code based on the first message authentication code and the first secret key using a third secret key. Prior art does not disclose or fairly teach f. transmitting the time stamp receipt, the first message authentication code, the second message authentication code, and the end key message to the requestor. Prior art does not disclose or fairly teach g. receiving at the outside agency at a second time a certification request, the certification request including the time stamp receipt, the first message authentication code, the second message authentication code, and the encrypted key message. Prior art does not disclose or fairly teach h. decrypting at the outside agency the encrypted key message to recover the first secret key. Prior art does not disclose or fairly teach i. validating the second message authentication code at the outside agency using the third secret key. Prior art does not disclose or fairly teach j. validating the first message authentication code at the outside agency using the first secret key if the second message authentication code is valid. Prior art does not disclose or fairly

Art Unit: 2131

teach k. certifying the time stamp receipt at the outside agency using a cryptographic signature scheme if the first message authentication code is valid.

Any claims not directly addressed are allowed on the virtue of their dependency.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
August 15, 2006

**CHRISTOPHER REVAK
PRIMARY EXAMINER**

CR 8/16/06